JOURNAL OF ALGEBRA **124**, 506–520 (1989)

Ideal Class Groups of Witt Rings

ROBERT W. FITZGERALD

Department of Mathematics, Southern Illinois University, Carbondale, Illinois 62901

Communicated by A. Fröhlich

Received August 11, 1987

This paper is, in part, a continuation of previous work on primary ideals of Witt rings [3]. There, for a formally real field F with finite height and only finitely many orderings, necessary and sufficient conditions were given for every ideal of the Witt ring WF containing an odd dimensional form to be principal. In this paper, the restriction on the height of F is dropped and the same conditions are shown to be equivalent to having every ideal which simply contains a non-zero-divisor be principal. This, in turn, can be shown to be equivalent to the ideal class group of the Witt ring being trivial. We are thus led to our main goal: computing the ideal class group of an arbitrary Witt ring.

The key to improving results from [3] is a theorem of Griffin [9] which states that WF is a Prufer ring unless F is Pythagorean with at least two orderings. This does not seem to have received the attention it deserves. Together with general properties of Prufer rings (many also due to Griffin), Griffin's theorem has many consequences for Witt rings, which we explore. These results complement primary decompositions nicely. We are thus able to prove a key lemma (1.8) by first deducing it for non-Pythagorean F since WF is Prufer, and then for Pythagorean F (when the height is 0, hence finite) since primary decompositions exist.

The first section reviews Griffin's results and applies them to Witt rings. The main result of this section extends work in [3] and [8] (by combining them). We show that for formally real F with only finitely many orderings, every ideal of WF containing an odd dimensional form is a (unique) product of prime ideals and has a (unique) primary decomposition.

The second section begins by discussing the main property of orderings required (weakly n-stable). Let X_F denote the set of orderings on F and $C(R)$ the ideal class group of the Witt ring $R = \mathrm{WF}$. We show that if $1 \leqslant |X_F| < \infty$ then $C(R)$ is trivial iff F is weakly 2-stable. More generally, suppose F is weakly n-stable but not weakly $(n-1)$-stable $(n \geqslant 3)$ and

0021-8693/89 $3.00

$|X_F| = r$. Then $C(R)$ is a finite group of 2-power order, each element of $C(R)$ has order at most 2^{n-2}, and $2^{n-2} \leqslant |C(R)| \leqslant 2^{(n-2)(r-1)}$.

Two noteworthy corollaries of these results (under the assumption $1 \leqslant |X_F| < \infty$) are (i) If an ideal $I \subset \mathrm{WF}$ contains a non-zero-divisor a then $I = (a, b)$ for some $b \in \mathrm{WF}$, and (ii) If F is n-stable and an ideal $I \subset \mathrm{WF}$ contains a non-zero-divisor then $I^{2^{n-2}}$ is principal.

The third section presents an example, namely the computation of the ideal class group of WF for $F = \mathbb{R}((t_1))((t_2)) \cdots ((t_n))$.

As was the case in [3], all of the arguments here are elementary. In particular, all of the results hold in a more general setting, such as that of the abstract Witt rings defined by Marshall [15].

Throughout F will denote a formally real field and R will denote the Witt ring of non-degenerate quadratic forms over F. IF will denote the ideal in R of even dimensional forms and I^nF the nth power of IF. We denote the natural numbers by $\mathbb{N}$ and $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$, by $\mathbb{Z}_n$. The set of orderings on F is X_F. For $m \in \mathbb{N}$, $m \geqslant 3$, and $\alpha \in X_F$ we let

$$P(\alpha) = \{r \in R \mid \operatorname{sgn}_\alpha r = 0\}$$

$$P(\alpha, m) = \{r \in R \mid \operatorname{sgn}_\alpha r \equiv 0 \pmod m\}.$$

The prime ideals of R are IF, $P(\alpha)$, $P(\alpha, p)$ as α ranges over X_F and p ranges over odd primes. Only the primes $P(\alpha)$ are not maximal. For these results and other basic results, terms, notation for Witt rings see [12].

We generally follow [4] for terminology and notation in multiplicative ideal theory. However, most of the basic terms are defined as needed in this paper. In several places results on orderings not found in [12] are needed. References to original papers are given as well as references to [13], which has a more uniform terminology (used here).

1. Regular Ideals

We begin by assembling some basic results (due primarily to Griffin) and definitions. An element $x \in R$ is a *regular element* if it is not a zero-divisor. An ideal $I \subset R$ is a *regular ideal* if it contains a regular element.

Lemma 1.1. (1) *If R is not reduced then $x \in R$ is regular* iff *x is odd dimensional.*

(2) *If R is reduced then $x \in R$ is regular* iff $\operatorname{sgn}_\alpha x \neq 0$ *for all* $\alpha \in X_F$.

Proof. [12, VIII 6.6]. ∎

If R is reduced we will need to distinguish those regular elements of R which are odd dimensional. We make the following:

DEFINITION. An element $x \in R$ is *strongly regular* if x is odd dimensional.

Thus strongly regular elements of R are regular and if R is not reduced then the converse holds. Note that our definition of strongly regular is *not* the same as in [7]. For commutative rings, the strongly regular elements of Goldie and Krause are precisely the regular elements.

K will denote the *total quotient ring* of R, that is, $K = S^{-1}R$ where $S = \{x \in R \mid x \text{ regular}\}$. An ideal $I \subset R$ is *invertible* if there exists an R-module $J \subset K$ with $IJ = R$. Invertible ideals are regular. A (commutative, with unity) ring S is a *Prufer ring* if every finitely generated regular ideal is invertible. The following is [9, Proposition 15]:

THEOREM 1.2. (Griffin). *R is a Prufer ring iff R is not reduced or if $R \approx \mathbb{Z}$.*

Griffin, in [8], has found many conditions on a ring S equivalent to S being Prufer. We list some of the more interesting ones for our Witt ring R:

THEOREM 1.3 (Griffin). *The following are equivalent:*

(1) *R is a Prufer ring.*

(2) *If P is a maximal ideal of R, I and J ideals of R with at least one regular, then either $IR_p \subset JR_p$ or $JR_p \subset IR_p$.*

(3) *Every over-ring S, $R \subset S \subset K$, is a flat R-module.*

(4) *If I, J, L are ideals of R with J or L regular, then $I(J \cap L) = IJ \cap IL$.*

(5) *If I and J are ideals of R, one of which is regular, then $(I+J)(I \cap J) = IJ$.*

(6) *If I and J are ideals of R with J finitely generated and regular and $I \subset J$ then $I = JL$, for some ideal $L \subset R$.*

COROLLARY 1.4. *Let R be non-reduced. Then*

(1) *R is integrally closed in K.*

(2) *If I, J, L are ideals of R with I regular, then $IJ = IL$ implies $J = L$.*

Proof. (1) is by [8, Theorem 13]. (2) follows from [8, Theorem 15] since each regular maximal ideal P yields a Manis valuation with $\mathbb{Z} \cup \infty$. To be more specific: let $P = P(\alpha, p)$, where $\alpha \in X_F$ and p is an odd prime. The signature map $\text{sgn}_\alpha: R \to \mathbb{Z}$ extends to a homomorphism $s: K \to \mathbb{Q}$. Let $v_p: \mathbb{Q} \to \mathbb{Z} \cup \infty$ be the usual p-adic valuation. Then $r = v_p \circ s: K \to \mathbb{Z} \cup \infty$ gives the required Manis valuation.

COROLLARY 1.5. *The following are equivalent:*

(1) *R is non-reduced and $|X_F| < \infty$, or $R \approx \mathbb{Z}$.*

(2) *All regular ideals of R are invertible.*

(3) *Every regular ideal of R is a product of prime ideals.*

Proof. (2) $\leftrightarrow$ (3) is [8, Theorem 17]. To show (1) $\leftrightarrow$ (2) it suffices, by [8, Theorem 17] and (1.4), to note that $|X_F| = \infty$ iff some regular element lies in infinitely many primes. For example, $3 \cdot \langle 1 \rangle \in P(\alpha, 3)$ for all $\alpha \in X_F$. ∎

The equivalence of (1) and (3) in (1.5) is closely related to work in [3] and can be used to extend its main theorem. [3, 2.3] said every ideal has a primary decomposition iff $|X_F| < \infty$ and $h(F) < \infty$. For strongly regular ideals the restriction on the height $h(F)$ can be dropped (cf. (1.8)).

We begin the work to extend some of the results of [3] to fields with infinite height and some of the results of [8] to reduced Witt rings.

LEMMA 1.6. *Let $\alpha \in X_F$ and let P be an odd prime. For any $k \in \mathbb{N}$, $P(\alpha, p^k) = P(\alpha, p)^k$.*

Proof. Clearly $P(\alpha, p)^k \subset P(\alpha, p^k)$ and $p^k \cdot \langle 1 \rangle \in P(\alpha, p)^k$. If $a <_\alpha 0$ then $\langle 1, a \rangle = \langle 1, a \rangle (\langle 1 \rangle \perp s\langle 1, -a \rangle)^k \in P(\alpha, p)^k$, where $s = (p-1)/2$. The elements $\langle 1, a \rangle$ with $a <_\alpha 0$ generate $P(\alpha)$. Thus $P(\alpha, p^k) = P(\alpha) + (p^k \cdot \langle 1 \rangle) \subset P(\alpha, p)^k$. ∎

We recall the primary ideals of R from [3]. Let $\alpha \in X_F$ and p be an odd prime. The only $P(\alpha)$-primary ideal is $P(\alpha)$. The $P(\alpha, p)$-primary ideals are $P(\alpha, p^k)$, $k \geq 1$, and the IF-primary ideals are all ideals $I \subset IF$ with $2^k \cdot \langle 1 \rangle \in I$ for some $k \geq 1$.

PROPOSITION 1.7. *Suppose $|X_F| < \infty$. If $Q_1, \ldots, Q_n$ are strongly regular primary ideals with distinct radicals then $\bigcap_{i=1}^n Q_i = \prod_{i=1}^n Q_i$.*

Proof. We first suppose that R is non-reduced (that is, F is non-Pythagorean). We use induction on n and consider first the case $n = 2$. Let $Q_1 = P(\alpha_1, p_1^{e_1})$ and $Q_2 = P(\alpha_2, p_2^{e_2})$ with, for $i = 1, 2$, $\alpha_i \in X_F$, p_i odd primes and $e_i \geq 1$. Our assumption on the radicals implies $\alpha_1 \neq \alpha_2$ or $p_1 \neq p_2$. In either case, $P(\alpha_1, p_1) + P(\alpha_2, p_2) = R$. By the Chinese Remainder Theorem and (1.6), $Q_1 + Q_2 = P(\alpha_2, p_1)^{e_1} + P(\alpha_2, p_2)^{e_2} = R$. Then $Q_1 \cap Q_2 = Q_1 Q_2$ by (1.3) (5). For $n > 2$ we have

$$\prod_{i=1}^{n} Q_i = Q_1 \prod_{i=2}^{n} Q_i = Q_1 \left(\bigcap_{i=2}^{n} Q_i \right), \qquad \text{by induction}$$

$$= \bigcap_{i=2}^{n} Q_1 Q_i, \qquad \text{by (1.3) (4)}$$

$$= \bigcap_{i=1}^{n} Q_i, \qquad \text{by the case } n = 2.$$

We now consider the reduced case. Here the height of F is 0 and so [3, 2.3] implies $\prod_{i=1}^{n} Q_i$ has a primary decomposition. Let $I = \prod_{i=1}^{n} Q_i$ and $J = \bigcap_{i=1}^{n} Q_i$. Clearly $I \subset J$. Let $Q_i = P(\alpha_i, p_i^{e_i})$, where $\alpha_i \in X_F$, p_i is an odd prime, and $e_i \geqslant 1$.

Let $Q = P(\beta, q^f)$ be a primary ideal containing I. We first show β is some α_i, $i = 1, ..., n$. Suppose not. Then for each $i = 1, ..., n$ we may choose $a_i \in F$ with $a_i <_{\alpha_i} 0$ and $a_i >_{\beta} 0$. Then $x = \prod_{i=1}^{n} \langle 1, a_i \rangle \in \prod_{i=1}^{n} Q_i = I \subset Q$, but $\operatorname{sgn}_{\beta} x = 2^n$, a contradiction. We may thus suppose $\beta = \alpha_1$. Say $\alpha_1 = \alpha_2 = \cdots = \alpha_r$ and $\alpha_1 \neq \alpha_i$ for $r < i \leqslant n$. Using the same a_i, set $y = \prod_{i=1}^{r} p_i^{e_i} \cdot \prod_{i=r+1}^{n} \langle 1, a_i \rangle$. Again $y \in \prod_{i=1}^{n} Q_i \subset Q$. Now $\operatorname{sgn}_{\beta} y = 2^{n-r} \cdot \prod_{i=1}^{r} p_i^{e_i}$ must thus be 0 modulo q^f. Hence q is some p_i, say p_1, and $f \leqslant e_1$. That is, $Q = P(\beta, q^f) = P(\alpha_1, p_1^f) \supset P(\alpha_1, p_1^{e_1}) = Q_1$.

We thus have that every primary ideal Q in a primary decomposition of I contains some Q_i, and hence Q contains $J = \bigcap_{i=1}^{n} Q_i$. So $J \subset \bigcap Q = I$ and we are done. ∎

We remark that we did not need the hypothesis $|X_F| < \infty$ in (1.7) when R was non-reduced.

The following extends [8, Theorem 17] and [3, 2.3].

THEOREM 1.8. *Suppose $|X_F| < \infty$ and let I be a strongly regular ideal of R. Then*

(1) *I is a unique (finite) product of prime ideals,*

(2) *I has a unique primary decomposition.*

Proof. If R is non-reduced then (1) follows from (1.5) and [5]. Powers of prime ideals $P(\alpha, p)^e$, are primary ideals by (1.6). So (2) follows from (1) and (1.7). If R is reduced, then (2) follows from [3, 2.3] and (2) implies (1) by (1.6) and (1.7). ∎

We remark that (1.8) fails if $|X_F| = \infty$. For R non-reduced, the failure of (1), hence (2) by (1.7), follows from (1.5). For R reduced, it is easy to check that $(3) = \bigcap_{\alpha \in X_F} P(\alpha, 3)$ does not have a primary decomposition if $|X_F| = \infty$. Hence (2) fails.

2. Ideal Class Groups

We begin by examining the key properties determining the structure of the ideal class group. The first two of the properties defined below were considered by Elman and Lam [2].

Definitions. (1) A field F is *i-stable* if $I^{i+1}F = 2I^iF$.

(2) A field F is *weakly i-stable* if for all disjoint closed sets A, $B \subset X_F$ there exists a form $q \in I^iF$ such that $\operatorname{sgn}_\alpha q = 0$ for $\alpha \in A$ and $\operatorname{sgn}_\beta q = 2^i$ for $\beta \in B$.

(3) A field F is *i-covered* if for all disjoint closed sets A, $B \subset X_F$ there exists a form $q \in R = WF$ such that $\operatorname{sgn}_\alpha q = 0$ for $\alpha \in A$ and $\operatorname{sgn}_\beta q = 2^i$ for $\beta \in B$.

In general, i-stable implies weakly i-stable [2, 3.7] and weakly i-stable implies i-covered. If $I^{i+1}F$ is torsion-free then i-stable and weakly i-stable are equivalent [2, 3.7]. We will show that weakly i-stable and i-covered are equivalent if $|X_F| < \infty$.

Lemma 2.1. *If $|X_F| < \infty$ then F is weakly i-stable for some $i \leqslant \max\{1, |X_F| - 1\}$.*

Proof. We may assume $|X_F| > 1$, since the case $|X_F| = 1$ is easy. Let $X_F = \{\alpha_0, ..., \alpha_r\}$. Let A and $B \subset X_F$ be disjoint (necessarily closed) subsets. For each $\beta \in B$ we can find an r-fold Pfister form p_β such that $\operatorname{sgn}_\alpha p_\beta = 0$ for $\alpha \neq \beta$ and $\operatorname{sgn}_\beta p_\beta = 2^r$ [3, 2.3]. Then $q = \sum_{\beta \in B} p_\beta$ is the element showing F is r-covered. ∎

Proposition 2.2. *Suppose $|X_F| < \infty$ and $i \geqslant 1$. Then F is weakly i-stable iff F is i-covered.*

Proof. We need to show that if F is i-covered then F is weakly i-stable. It is enough to do this for Pythagorean F. Namely, if $T = \sum \dot{F}^2$ then by [14] there exists a Pythegorean field K with $\dot{F}/T \approx \dot{K}/\dot{K}^2$. Further, if we write $(aT)^*$ for the image of aT in $\dot{K}/\dot{K}^2$ then $X_K = \{\alpha^* \mid \alpha \in X_F\}$, where $\alpha^*(aT)^* = 1$ iff $\alpha(a) = 1$. Thus F is i-covered iff K is i-covered and F is weakly i-stable iff K is.

We may thus assume F is Pythagorean and $|X_F| < \infty$. Let A and B be disjoint subsets of X_F. Extend A to $A' = X_F \setminus B$. We know there exists $q \in R = \mathrm{WF}$ such that $\operatorname{sgn}_\alpha q = 0$ if $\alpha \notin B$ and $\operatorname{sgn}_\alpha q = 2^i$ if $\alpha \in B$. In particular, $2^i \mid \operatorname{sgn}_\alpha q$ for all $\alpha \in X_F$. By [15, 8.20] $q \in I^iF$. Hence F is weakly i-stable. ∎

Recall that for $\alpha \in X_F$, $m \in \mathbb{N}$, $m \geqslant 3$, we let $P(\alpha, m)$ denote $\{r \in R \mid$

$\operatorname{sgn}_\alpha r \equiv 0 \pmod m\}$. Note that if $m = \prod_{i=1}^n p_i^{e_i}$, where $p_1, \ldots, p_n$ are distinct odd primes, then $P(\alpha, m) = \bigcap_{i=1}^n P(\alpha, p_i^{e_i})$. We also recall (1.6): $P(\alpha, p_i^{e_i}) = P(\alpha, p_i)^{e_i}$.

LEMMA 2.3. *Suppose* $|X_F| < \infty$ *and* $i \geq 2$. *The following are equivalent*:

(1) F *is weakly* i*-stable.*

(2) $P(\alpha, m)$ *is principal for all* $\alpha \in X_F$ *and all* $m \equiv \pm 1 \pmod{2^i}$.

(3) $P(\alpha, 2^i + 1)$ *is principal for all* $\alpha \in X_F$.

Proof. (1) $\rightarrow$ (2): Write $m = 1 + k \cdot 2^i$ (the case $m \equiv -1 \pmod{2^i}$ is similar) and fix $\alpha \in X_F$. By assumption, there is a form q such that $\operatorname{sgn}_\beta q = 0$ if $\beta \neq \alpha$ and $\operatorname{sgn}_\alpha q = 2^i$. Set $\sigma = \langle 1 \rangle + kq$. We consider the primary decomposition of (σ). Let $Q = P(\beta, p^j)$ be a primary ideal containing σ. Since $\operatorname{sgn}_\beta \sigma = 1$ if $\beta \neq \alpha$, we must have $\beta = \alpha$. Further, $\operatorname{sgn}_\alpha \sigma = m \equiv 0 \pmod{p^j}$. Thus if $m = \prod_{i=1}^n p_i^{e_i}$ is a prime factorization, p equals some p_i and $j \leq e_i$. Thus the ideals $P(\alpha, p_i^{e_i})$ are the minimal primary ideals containing σ. By (1.8), $(\sigma) = \bigcap_{i=1}^n P(\alpha, p_i^{e_i}) = P(\alpha, m)$.

(2) $\rightarrow$ (3) is trivial.

(3) $\rightarrow$ (1): Fix $\alpha \in X_F$ and set $m = 1 + 2^i$. We will show there is a form $\sigma \in R = \mathrm{WF}$ with $\operatorname{sgn}_\beta \sigma = 0$ if $\beta \neq \alpha$ and $\operatorname{sgn}_\alpha \sigma = 2^i$, which is sufficient by (2.2). We have $P(\alpha, m) = (q)$ for some form q. Then $\operatorname{sgn}_\alpha q = \pm m$ and if $\beta \neq \alpha$, $\operatorname{sgn}_\beta q = \pm 1$ (otherwise there is a primary ideal containing (σ) but not $P(\alpha, m)$). By multiplying by -1 if necessary, we may assume $\operatorname{sgn}_\alpha q = m$. Further, there is an element $a \in \dot{F}$ represented by q with $a >_\alpha 0$. So replacing q by aq if necessary, we may assume $q \simeq \langle 1 \rangle + q_0$ for some form q_0.

If $\operatorname{sgn}_\beta q_0 = 0$ for all $\beta \neq \alpha$ then we are done. So suppose otherwise. Then there exists a $\beta \in X_F$ with $\operatorname{sgn}_\beta q_0 = -2$ (since $\operatorname{sgn}_\beta q = \pm 1$ for all $\beta \neq \alpha$ and $q_0 = q - \langle 1 \rangle$). In particular, $q_0 \in IF \setminus I^2F$. We may write $q_0 = \langle b, bd \rangle + q_1$, with some $q_1 \in I^2F$. Set $q_2 = \langle\langle b, d \rangle\rangle + q_1$. We will show $\operatorname{sgn}_\beta q_2 = 0$ for $\beta \neq \alpha$ by considering various cases.

Case 1. $\operatorname{sgn}_\beta q_0 = 0$.

Here $\operatorname{sgn}_\beta \langle b, bd \rangle = -\operatorname{sgn}_\beta q_1 \equiv 0 \pmod 4$, since $q_1 \in I^2F$. Hence $\operatorname{sgn}_\beta \langle b, bd \rangle = 0$. Thus $\operatorname{sgn}_\beta \langle\langle b, d \rangle\rangle = 0$ and $\operatorname{sgn}_\beta q_2 = \operatorname{sgn}_\beta q_1 = \operatorname{sgn}_\beta q_0 = 0$.

Case 2. $\operatorname{sgn}_\beta q_0 = -2$.

Since 4 divides $\operatorname{sgn}_\beta q_1$, we have that $\operatorname{sgn}_\beta \langle b, bd \rangle = \pm 2$. Suppose first that $\operatorname{sgn}_\beta \langle b, bd \rangle = 2$. Then $\operatorname{sgn}_\beta q_1 = -4$ and $\operatorname{sgn}_\beta \langle\langle b, d \rangle\rangle = 4$. Thus $\operatorname{sgn}_\beta q_2 = 0$. Next suppose that $\operatorname{sgn}_\beta \langle b, bd \rangle = -2$. Then $\operatorname{sgn}_\beta q_1 = 0$ and $\operatorname{sgn}_\beta \langle\langle b, d \rangle\rangle = 0$. Thus again $\operatorname{sgn}_\beta q_2 = 0$.

We thus have $\operatorname{sgn}_\beta q_2 = 0$ for all orderings $\beta \neq \alpha$. Lastly, $\operatorname{sgn}_\alpha \langle b, bd \rangle \equiv -\operatorname{sgn}_\alpha q_1 \pmod{2^i}$, since $\operatorname{sgn}_\alpha q_0 = \operatorname{sgn}_\alpha(\langle b, bd \rangle + q_1) = 2^i$. Then

$\operatorname{sgn}_\alpha\langle b, bd\rangle \equiv 0 \pmod 4$ since $q_1 \in I^2F$ and $i \geq 2$. Hence $\operatorname{sgn}_\alpha\langle b, bd\rangle = 0$, $\operatorname{sgn}_\alpha\langle\langle b, d\rangle\rangle = 0$ and $\operatorname{sgn}_\alpha q_2 = \operatorname{sgn}_\alpha q_1 = \operatorname{sgn}_\alpha q - 1 = 2^i$, as desired. ∎

We may now extend [9, Proposition 15] to strongly regular ideals in reduced Witt rings.

COROLLARY 2.4. *If $|X_F| < \infty$ then every strongly regular ideal is invertible.*

Proof. If R is not reduced then this is (1.5). If R is reduced then any strongly regular ideal is a product of prime ideals (1.8). So it is enough to show that strongly regular prime ideals are invertible. Let $I = P(\alpha, p)$, where $\alpha \in X_F$ and p is an odd prime. F is weakly i-stable for some i (2.1). Let e denote the order of p in the group of units in $\mathbb{Z}_{2^i}$. Then $p^e \equiv 1 \pmod{2^i}$ and $I^e = P(\alpha, p^e)$ is principal by (2.3). Hence I is invertible. ∎

If R is not reduced, and X_F is finite, then the notions of regular ideals, strongly regular ideals, and invertible ideals coincide. However, if R is reduced then there may exist regular ideals that are not invertible and invertible ideals that are not strongly regular.

Indeed, if R is reduced, $R \not\cong \mathbb{Z}$, and X_F finite then (1.5) implies there must exist regular ideals that are not invertible. If $|\dot{F}/\dot{F}^2| > 4$ then IF is such an ideal. And for any reduced ring R, the principal ideal (2) is invertible but not strongly regular. To give an example of a non-principal, invertible ideal that is not strongly regular, let $F = \mathbb{R}((t_1))((t_2))((t_3))$. Set $I = (4, 2 - \langle\langle t_1, t_2, t_3\rangle\rangle)$. I is not principal since if q were a generator then q would have signature ± 2 at each ordering. Further, q divides $2 - \langle\langle t_1, t_2, t_3\rangle\rangle$ with quotient q' having signature ± 3 when $t_1, t_2, t_3 > 0$ and ± 1 at all other orderings. But then $P(\alpha, 3) = (q')$, which is impossible [3, p. 380]. However, $I^2 = (16, 8 - 4\langle\langle t_1, t_2, t_3\rangle\rangle, 4 + 4\langle\langle t_1, t_2, t_3\rangle\rangle) = (4)$. Thus I is invertible, but not strongly regular.

PROPOSITION 2.5. *Suppose $|X_F| < \infty$ and let I be an invertible ideal of R. If $a \in I$ is regular then $I = (a, b)$ for some $b \in R$.*

In particular, every ideal containing an odd dimensional form a can be generated by a and some $b \in R$.

Proof. The second statement follows from the first. If an ideal I contains an odd dimensional form a then, by definition, I is strongly regular and hence invertible (2.4). The first statement then yields the second since a is regular.

The first statement follows from [6, Theorem 3] if we can show that a is contained in only finitely many maximal ideals of R. Suppose otherwise. Then, since $|X_F| < \infty$, $a \in P(\alpha, p)$ for some $\alpha \in X_F$ and infinitely many

primes p. Thus, $a \in P(\alpha)$. But then a is even dimensional and $\operatorname{sgn}_\alpha a = 0$, which contradicts (1.1). ∎

We review the construction of the ideal class group. K will again denote the total quotient ring of R. A *fractional ideal* of R is an R-submodule I of K such that $rI \subset R$ for some regular element $r \in R$. Note that rI is an ideal of R. A fractional ideal I is *invertible* if there exist a fractional ideal J such that $IJ = R$. Note that if I is an invertible fractional ideal with $rI \subset R$ then rI is an invertible ideal of R (as defined earlier). The set $I(R)$ of all invertible fractional ideals of R is a group under multiplication. The set of principal regular fractional ideals of R forms a subgroup $P(R)$ of $I(R)$. The factor group $I(R)/P(R)$ is the *ideal class group* of R, denoted $C(R)$. If I is an invertible fractional ideal of R then $[I]$ will denote the coset $IP(R) \in C(R)$. Note that an element of $C(R)$ may be represented by $[I]$, where I is an invertible (hence regular) ideal of R.

The key to calculating $C(R)$, for a Witt ring R, is the following better representation.

LEMMA 2.6. *Suppose* $|X_F| < \infty$. *Then any element* $x \in C(R)$ *may be represented as* $x = [J]$, *where* J *is a strongly regular ideal of* R.

Proof. We may assume $x = [I]$, where I is an invertible ideal of R. If $I \not\subset IF$ then I is strongly regular, so we may assume $I \subset IF$. Then $I_{IF} = (a)_{IF}$ for some form $a \in I$ [4, 17.3, 7.4]. Indeed, a must be regular since I is [4, 17.1]. Then by (2.5), $I = (a, b)$, for some form $b \in R$. Now $b/1 \in I_{IF} = (a)_{IF}$, so $b/1 = ay/z$, for some $y \in R$ and $z \in R \setminus IF$. That is, $bx = ay$. Hence

$$(z)(a, b) = (az, ay) = (a)(z, y).$$

Set $J = (z, y)$. J is strongly regular since z is and so J is invertible by (2.4). Clearly $[I] = [J]$ in $C(R)$. ∎

We may now extend (3.1) of [3].

THEOREM 2.7. *Suppose* $|X_F| < \infty$. *Then* $C(R) = \{1\}$ *iff* F *is weakly 2-stable. In this case, there is unique factorization into irreducibles for regular forms.*

Proof. $C(R) = \{1\}$ iff every strongly regular ideal is principal by (2.6). The result thus follows from [3, 3.1]. (Note: Theorem 3.1 of [3] has the additional assumption that the height $h(F)$ is finite. The proof of (3.1) only uses this extra assumption to ensure the existence of primary decompositions, which now follows from (1.8)). ∎

We now compute $C(R)$ in general. We first observe that for m and n odd, $P(\alpha, m)\, P(\alpha, n) = P(\alpha, mn)$, which can be easily deduced from (1.7).

THEOREM 2.8. *Suppose F is weakly i-stable but not weakly $(i-1)$-stable, where $i \geq 3$. Suppose also that $|X_F| < \infty$. For each $\alpha \in X_F$ let $H(\alpha) = \{[P(\alpha, m)] \mid m \text{ an odd integer}\} \subset C(R)$. Then:*

(1) *$H(\alpha)$ is a subgroup of $C(R)$.*

(2) *$|H(\alpha)| = 2^j$, for some $j \leq i-2$.*

(3) *$H(\alpha)$ is cyclic, generated by $[P(\alpha, 5)]$.*

(4) *There exists $\alpha \in X_F$ with $|H(\alpha)| = 2^{i-2}$.*

Proof. Let $^- : \mathbb{Z} \to \mathbb{Z}_{2^i}$ and let $G = U(\mathbb{Z}_{2^i})/\{\pm 1\}$. For an odd integer m let $\bar{\bar{m}}$ denote its image in G. It is well known (cf. [10, IV Theorem 2']) that G is cyclic of order 2^{i-2} and generated by $\bar{\bar{5}}$.

Consider the map $\chi : U(\mathbb{Z}_{2^i}) \to C(R)$ defined by $\chi(\bar{m}) = [P(\alpha, m)]$. χ is well-defined. Namely, if $\bar{n} = \bar{m} \in U(\mathbb{Z}_{2^i})$, let $\bar{k} = \bar{n}^{-1} = \bar{m}^{-1}$; then $mk \equiv nk \equiv 1 \pmod{2^i}$. Hence by (2.3) $[P(\alpha, n)][P(\alpha, k)] = [P(\alpha, nk)] = 1$, and $[P(\alpha, m)][P(\alpha, k)] = 1$. Thus $[P(\alpha, n)] = [P(\alpha, m)]$. Also, χ is clearly a group homomorphism.

Since the image of χ is $H(\alpha)$, $H(\alpha)$ is a group. Also, $P(\alpha, 1) = P(\alpha, -1) = R$, so $\{\pm 1\}$ is in the kernel of χ. We thus get a surjective homomorphism $\chi_1 : G \to H(\alpha)$. Parts (2) and (3) now follow from the first paragraph.

To prove (4), suppose the result is false, that is, suppose $|H(\alpha)| \leq 2^{i-3}$ for all $\alpha \in X_F$. Fix $a \in X_F$. The map χ_1 is not injective and so contains an element of order 2, say g. Now $(2^{i-1}+1)^2 \equiv 1 \pmod{2^i}$ and $2^{i-1}+1 \not\equiv \pm 1 \pmod{2^i}$ since $i \geq 3$. Set $m = 2^{i-1}+1$. Then $\bar{\bar{m}}$ has order 2 in G, and since G is cyclic, $\bar{\bar{m}} = g$. Thus $1 = \chi_1(\bar{\bar{m}}) = [P(\alpha, m)]$. That is, $P(\alpha, m)$ is principal. This holds for each $\alpha \in X_F$. Then (2.3) implies that F is weakly $(i-1)$-stable, a contradiction. ∎

COROLLARY 2.9. *Let F be weakly i-stable but not weakly $(i-1)$-stable, with $i \geq 3$. Let $X_F = \{\alpha_1, \ldots, \alpha_r\}$. Then*

(1) *$C(R) = \prod_{i=1}^{r} H(\alpha_i)$, where $H(\alpha)$ is as in (2.8).*

(2) *$C(R)$ is a finite group of 2-power order.*

(3) *Every element of $C(R)$ has order at most 2^{i-2}.*

(4) *$2^{i-2} \leq |C(R)| \leq 2^{(i-2)(r-1)}$.*

Proof. Let $x \in C(R)$. Then $x = [J]$ for some strongly regular ideal J of R by (2.6). J is a product of maximal ideals of the form $P(\alpha, p)$ by (1.8). Hence $x = [J]$ lies in the product of some $H(\alpha)$'s. Thus (1) holds. Statements (2) and (3) now follow from (2.8) (2). Lastly, note that $(5) = \bigcap_{i=1}^{r} P(\alpha_i, 5) = \prod_{i=1}^{r} P(\alpha_i, 5)$, by (1.7). Hence $H(\alpha_r) \subset H(\alpha_1) \cdot \cdots \cdot$

$H(\alpha_{r-1})$, by (2.8) (3). Since at least one $H(\alpha)$ has order 2^{i-2} (by (2.8) (4)) and generally $|H(\alpha)| \leqslant 2^{i-2}$, statement (1) yields (4). ∎

COROLLARY 2.10. *Suppose* $|X_F| < \infty$ *and* F *is weakly* i*-stable. Then for any invertible ideal* I, $I^{2^{i-2}}$ *is principal.*

Proof. Immediate from (2.9) (3). ∎

3. EXAMPLE

We compute $C(R)$ in the case $F = \mathbb{R}((t_1))((t_2))\cdots((t_n))$. Here the Witt ring R is the group ring $\mathbb{Z}[\Delta_n]$, where Δ_n is the elementary 2-group with basis $t_1, \ldots, t_n$. The basic fact about the set of orderings we need is that every subgroup $T \subset \dot{F}/\dot{F}^2$, that does not contain -1, is a fan ([2, 4.6], cf. also [13, p. 45]).

THEOREM 3.1. *Let* $n \geqslant 3$. *Then*

$$C(\mathbb{Z}[\Delta_n]) \approx \bigotimes_{i=1}^{n-2} (\mathbb{Z}_{2^i})^{\binom{n}{i+2}}.$$

The proof of (3.1) requires several lemmas and considerable notation.

LEMMA 3.2. *F is weakly n-stable but not weakly $(n-1)$-stable.*

Proof. Since F is Pythagorean, weakly n-stable is equivalent to n-stable [2, 3.7]. The result thus follows from [2, p. 1178]. ∎

In the cases omitted from (3.1), namely $n = 0, 1, 2$, we have $C(\mathbb{Z}[\Delta_n]) = \{1\}$ by (3.2) and (2.7). Also we note that for $n \geqslant 3$, $\log_2 |C(\mathbb{Z}[\Delta_n])| = \sum_{i=1}^{n-1} i\binom{n}{i+2}$. The case $n = 3$ yields $|C(\mathbb{Z}[\Delta_3])| = 2$, showing that the lower bound of (2.9) is the best possible. However, in no case is $|C(\mathbb{Z}[\Delta_n])|$ as large as the upper bound of (2.9).

For a prime p and integer z, we let $p \parallel z$ denote as usual $p^n \mid z$ and $p^{n+1} \nmid z$.

LEMMA 3.3. $m \in \mathbb{N}$, $2^{m+2} \parallel 5^{2^m} - 1$.

Proof. This is a restatement of [10, IV Theorem 2′] and easy to prove directly by induction.

We introduce some more notation: For $\alpha \in X_F$ let $i(\alpha) = |\{t_j \mid t_j >_\alpha 0\}|$. Set $S_j = \{\alpha \in X_F \mid i(\alpha) = j\}$ and $G_j = \prod_{\alpha \in S_j} H(\alpha)$, where $H(\alpha)$ is defined as in (2.8).

LEMMA 3.4. $C(R) = \prod_{j=3}^{n} G_j$.

Proof. $C(R) = \prod_{\alpha \in X_F} H(\alpha) = \prod_{j=0}^{n} G_j$ by (2.9). Let $G' = \prod_{j=3}^{n} G_j$. Pick $\beta \in S_2$. Then for some $i \neq j$, $t_i >_\beta 0$ and $t_j >_\beta 0$. We have, using primary decomposition and (1.7),

$$(1 + \langle\langle t_i, t_j \rangle\rangle) = \prod_{\gamma \in T} P(\gamma, 5),$$

where $T = \{\gamma \in X_F \mid t_i >_\gamma 0,\ t_j >_\gamma 0\}$. Clearly $T \setminus \{\beta\} \subset \bigcup_{j=3}^{n} S_j$. Hence $[P(\beta, 5)] = \prod_{\gamma \in T \setminus \{\beta\}} [P(\gamma, 5)]^{-1} \in G'$. Thus $H(\beta) \subset G'$ and $G_2 \subset G'$.

Now let $\beta \in S_1$ with, say, $t_i >_\beta 0$. Then $(1 + \langle\langle 1, t_i \rangle\rangle) = \prod_{\gamma \in U} P(\gamma, 5)$, where $U = \{\gamma \in X_F \mid t_i >_\gamma 0\}$. Since $U \setminus \{\beta\} \subset \bigcup_{j=2}^{n} S_j$, we obtain $[P(\beta, 5)] \in G_2 \cdot G' \subset G'$ and so $G_1 \subset G'$. Lastly, say $S_0 = \{\beta\}$. From $(5) = \prod_{\gamma \in X_F} P(\gamma, 5)$ we see that $G_0 \subset G_1 G_2 G' \subset G'$. Hence $G = G_0 G_1 G_2 G' \subset G'$. The inclusion $G' \subset G$ is obvious, so we obtain $G' = G$. ∎

Let K be a subgroup of $\dot{F}/\dot{F}^2$ of index 2^k $(k \geqslant 2)$ such that $-1 \notin K$. Since K is a fan, the set of orderings for which K is positive has $r = 2^{k-1}$ elements, say $A = \{\alpha_1, ..., \alpha_r\}$. Denote by $x(K)$ the product $\prod_{\alpha \in A} [P(\alpha, 5)] \in C(R)$.

LEMMA 3.5. *Let K, A, and $x(K)$ be as above. Then the order of $x(K)$ in $C(R)$ is 2^{n-k-1}.*

Proof. Let $a_1, ..., a_s$ $(s = n - k + 1)$ be a $\mathbb{Z}_2$-basis for K. There exists $m \in \mathbb{N}$ with $m \cdot 2^s + 1 = 5^{2^{s-2}}$ by (3.3). Let $q = \langle 1 \rangle + m\langle\langle a_1, ..., a_s \rangle\rangle$. Then $\operatorname{sgn}_\alpha q = 1$ if $\alpha \notin A$ and $\operatorname{sgn}_\alpha q = 5^{2^{s-2}}$ if $\alpha \in A$. Taking the primary decomposition for (q) and using (1.7) yields $(q) = \prod_{\alpha \in A} P(\alpha, 5)^{2^{s-2}}$. Thus $x(K)^{2^{s-2}} = 1$, that is, $o(x(K)) \mid 2^{n-k-1}$.

Suppose then that $x(K)^{2^{n-k-2}} = 1$. Then there exists $q' \in R$ such that $\operatorname{sgn}_\alpha q' = \pm 1$ if $\alpha \notin A$ and $\operatorname{sgn}_\alpha q' = \pm 5^{2^{n-k-2}}$ if $\alpha \in A$. Let $e = d \pm (q')$. Then for $\alpha \notin A$, $\operatorname{sgn}_\alpha(eq') = 1$ by [11, p. 153].

We use a special case of a theorem of Brown [1] (cf. [13, 6.8]), namely this theorem applied to the fan $\dot{F}^2$:

$$\sum_{\alpha \in X_F} \operatorname{sgn}_\alpha(eq') \equiv 0 \pmod{2^n}.$$

If v denotes the number of α in A with $\operatorname{sgn}_\alpha(eq') > 0$, we obtain

$$v \cdot 5^{2^{n-k-2}} - (2^{k-1} - v)\, 5^{2^{n-k-2}} + (2^n - 2^{k-1}) \equiv 0 \pmod{2^n},$$

$$2v5^{2^{n-k-2}} - 2^{k-1}(5^{2^{n-k-2}} + 1) \equiv 0 \pmod{2^n}.$$

Now $2^k \mid 2^{k-1}(5^{n-k-2}+1)$ so $2^k \mid 2v$. But $v \leqslant |A| = 2^{k-1}$. Hence $v = 2^{k-1}$ and we obtain

$$2^{k-1}(5^{2^{n-k-2}}-1) \equiv 0 \pmod{2^n},$$

$$5^{2^{n-k-2}}-1 \equiv 0 \pmod{2^{n-k+1}}.$$

But $2^{n-k} \parallel 5^{2^{n-k-2}}-1$ by (3.3), which gives a contradiction. Hence the order of $x(K)$ is 2^{n-k-1}.

We introduce yet more notation. Recall that S_{n-1} is the set of orderings in which exactly one t_i is negative. S_{n-1} has n orderings, say $S_{n-1} = \{\alpha_1, ..., \alpha_n\}$. Let α_0 be the ordering in which all t_i are positive. Let $\mathrm{pc}(\alpha)$, for $\alpha \in X_F$, be the positive cone of α, that is, $\mathrm{pc}(\alpha) = \{a \in \dot{F}/\dot{F}^2 \mid a >_\alpha 0\}$.

For each subset $\{\alpha_{i_1}, ..., \alpha_{i_j}\}$ of S_{n-1}, with $1 \leqslant j \leqslant n-3$, let $K(i_1, ..., i_j) = \mathrm{pc}(\alpha_0) \cap \bigcap_{k=1}^{j} \mathrm{pc}(\alpha_{i_k})$. Let $x_0 = [P(\alpha, 5)] \in C(R)$ and $x(i_1, ..., i_j) = x(K(i_1, ..., i_j))$.

We make some preliminary remarks. $K(i_1, ..., i_j)$ is a subgroup of $\dot{F}/\dot{F}^2$ of index 2^{j+1}. Hence, by (3.5), the order of $x(i_1, ..., i_j)$ is 2^{n-j-2}. The order of x_0 is 2^{n-2} by (2.8). There are $\binom{n}{j}$ subsets of j orderings in S_{n-1} and so $\binom{n}{j}$ $x(i_1, ..., i_j)$'s for each j. Therefore, the direct product of the cyclic groups generated by the x's is isomorphic to $\bigotimes_{j=0}^{n-3} (\mathbb{Z}_{2^{n-j-2}})^{\binom{n}{j}}$, which is $\bigotimes_{i=1}^{n-2} (\mathbb{Z}_{2^i})^{\binom{n}{i+2}}$ upon setting $i = n-j-2$. Thus to prove (3.1) we need to show that $C(R)$ is the direct product of the cyclic subgroups generated by the x's.

Now $K(i_1, ..., i_j)$ will contain $(n-j)$ t_i's, say $t_1, ..., t_{n-j}$. Then $x(i_1, ..., i_j) = \prod_\alpha [P(\alpha, 5)]$ over all α with $t_i >_\alpha 0$, $1 \leqslant i \leqslant n-j$. In particular, there is exactly one α in the product with $i(\alpha) = n-j$ and all other α have $i(\alpha) > n-j$.

Proof of (3.1): We need to show, as remarked above, that $C(R)$ is generated by x_0 and the $x(i_1, ..., i_j)$ with $1 \leqslant j \leqslant n-3$ and that there are no relations among these x's.

Suppose the group H generated by the x's is not all of $C(R)$. Now H does contain $x_0 = [P(\alpha_0, 5)]$. Let k be the greatest integer such that H does not contain some $[P(\alpha, 5)]$ with $i(\alpha) = k$. We have that $3 \leqslant k < n$ by (3.4). We may suppose $t_1, ..., t_k$ are positive with respect to α. Let $\alpha_{i_1}, ..., \alpha_{i_j}$ be all the orderings in S_{n-1} for which $t_1, ..., t_k$ are positive. Note that $0 < j \leqslant n-3$, since $3 \leqslant < n$. Then $x(i_1, ..., i_j) = [P(\alpha, 5)] \cdot \prod_\beta [P(\beta, 5)]$, where $i(\beta) > k$ for all β in the second product. By the maximality of k, $\prod_\beta [P(\beta, 5)] \in H$. Since $x(i_1, ..., i_j) \in H$, we obtain $[P(\alpha, 5)] \in H$, a contradiction. Therefore $C(R)$ is generated by the x's.

Now suppose there is a relation among the x_0, $x(i_1, ..., i_j)$ where

$1 \leqslant j \leqslant n-3$. Let $x(i_1, ..., i_j)^n$ be a term in the relation with maximal j. We will show $x(i_1, ..., i_j)^n = 1$ in $C(R)$, thereby arriving at a contradiction.

Writing each x in the relation as a product of $[P(\alpha, 5)]$'s gives an equation in $C(R)$ of the form $\prod_{\alpha \in A} [P(\alpha, 5)]^{n_\alpha} = 1$. Thus there exists a form $q \in R$ with $(q) = \prod_{\alpha \in A} P(\alpha, 5^{n_\alpha})$. For this q, $\operatorname{sgn}_\alpha q = \pm 5^{n_\alpha}$ if $\alpha \in A$ and $\operatorname{sgn}_\alpha q = \pm 1$ if $\alpha \notin A$. By [11, p. 153], we may in fact assume that $\operatorname{sgn}_\alpha q = 1$ if $\alpha \notin A$.

For convenience of notation, suppose that $t_1, ..., t_r$ are precisely the t_i's in $K(i_1, ..., i_j)$. Let β be the ordering for which $t_1, ..., t_r$ are positive and $t_{r+1}, ..., t_n$ are negative. Then $x(i_1, ..., i_j) = [P(\beta, 5)] \prod_\alpha [P(\alpha, 5)]$ over some α with $i(\alpha) > r$. Note that the maximality of j implies that the only occurrence of $[P(\beta, 5)]$ in the equation $\prod_{\alpha \in A} [P(\alpha, 5^{n_\alpha})] = 1$ arises from its occurrence in $x(i_1, ..., i_j)^n$ in the original relation. In particular, the n_β in $(q) = \prod_{\alpha \in A} P(\alpha, 5^{n_\alpha})$ equals n, the power of $x(i_1, ..., i_j)$ in the relation.

Let C be the subgroup of $\dot{F}/\dot{F}^2$ generated by $-t_{r+1}, ..., -t_n$. Then applying Brown's theorem [1] (cf. [13, 6.8]) yields

$$\sum_{\alpha \in B} \operatorname{sgn}_\alpha q \equiv 0 \pmod{2^r},$$

where $B = \{\alpha \in X_F \mid C >_\alpha 0\}$. Now B consists of β and orderings α in which $t_{r+1}, ..., t_n$ and at least one other t_i are negative (that is, $i(\alpha) < r$). By the maximality of j, if $\alpha \in A$ then $i(\alpha) \geqslant r$. Hence $A \cap B = \{\beta\}$. Thus we have

$$\pm 5^n + (2^r - 1) \equiv 0 \pmod{2^r}.$$

Thus $\operatorname{sgn}_\beta q = 5^n$ and $5^n - 1 \equiv 0 \pmod{2^r}$. Write $m \cdot 2^r + 1 = 5^n$ for some $m \in \mathbb{N}$. Then $(\langle 1 \rangle + \dot{m} \ll t_1, ..., t_r \gg) = \prod_\alpha P(\alpha, 5^n)$ over α in which $t_1, ..., t_r >_\alpha 0$. Hence in $C(R)$, $1 = \prod_{\{\alpha \mid K(i_1, ..., i_j) >_\alpha 0\}} P(\alpha, 5^n) = x(i_1, ..., i_j)^n$ as desired. ∎

References

1. R. Brown, Superpythagorean fields, *J. Algebra* **42** (1976), 483–494.
2. R. Elman and T. Y. Lam, Quadratic forms over formally real fields and Pythagorean fields, *Amer. J. Math.* **94** (1972), 1155–1194.
3. R. Fitzgerald, Primary ideals in Witt rings, *J. Algebra* **96** (1985), 368–385.
4. R. Gilmer, "Multiplicative Ideal Theory," Dekker, New York, 1972.
5. R. Gilmer, On factorization into prime ideals, *Comment. Math. Helv.* **47** (1972), 70–74.
6. R. Gilmer and W. Heinzer, On the number of generators of an invertible ideal, *J. Algebra* **14** (1970), 139–151.
7. A. Goldie and G. Krause, Strongly regular elements of Noetherian rings, *J. Algebra* **91** (1984), 410–429.
8. M. Griffin, Prufer rings with zero divisors, *J. Reine Angew. Math.* **239** (1969), 55–67.
9. M. Griffin, Valuations and Prufer rings, *Canad. J. Math.* **26** (1974), 412–429.

10. K. IRELAND AND M. ROSEN, "A Classical Introduction to Modern Number Theory," Graduate Texts in Mathematics, No. 84, Springer-Verlag, New York/Berlin, 1982.
11. M. KNEBUSCH, A. ROSENBERG, AND R. WARE, Structure of Witt rings and quotients of abelian group rings, *Amer. J. Math.* **94** (1972), 119–155.
12. T. Y. LAM, "The Algebraic Theory of Quadratic Forms," Benjamin, Reading, MA., 1973.
13. T. Y. LAM, "Orderings, Valuations and Quadratic Forms," CBMS Regional Conference Series in Math, No. 52, Cont. Bd. Math. Sci., Washington, DC, 1983.
14. M. MARSHALL, Classification of finite spaces of orderings, *Canad. J. Math.* **31** (1979), 320–330.
15. M. MARSHALL, "Abstract Witt Rings," Queen's Papers in Pure and Applied Mathematics, Vol. 57, Queen's Univ. Kingdom, ON, 1980.